

CLAIMS

1. A method for filtering certificates issued from one or more certificate authorities (CA), the method comprising the steps of:

receiving a certificate and storing the certificate;

5 preventing use of the certificate until validation;

identifying a certificate authority that has issued the certificate;

identifying a certificate authority filter by referring to a table, that comprises identification of at least one certificate authority filter;

10 sending a request to the identified certificate authority filter;

receiving from the certificate authority filter a response to the request, the response comprising information related to the certificate authority that has issued the certificate and a public key of the certificate authority that has issued the certificate;

determining according to the response whether the certificate authority is a trusted certificate authority; and

15 20 validating the certificate if the certificate authority that has issued the certificate is a trusted certificate authority.

2. The method according to claim 1 further comprising the step of:

discarding the certificate if the response indicates that the certificate authority that has issued the certificate is not a trusted certificate authority.

3. The method according to claim 1, wherein the step of identifying the certificate authority that has issued the certificate comprises the further step of:

retrieving an identification of the certificate authority from the certificate.

4. The method according to claim 1, wherein the step of sending a request to the identified certificate authority filter comprises the further step of:

including in said request an identification of the certificate authority that has issued the certificate.

5. The method according to claim 1,

wherein the response received from the certificate authority filter comprises a level of trust assigned to the certificate authority, and

wherein the step of determining according to the response whether the certificate authority is a trusted certificate authority comprises the further step of:

checking whether the level of trust assigned to the certificate authority corresponds to a level of trust of a trusted certificate authority.

6. The method according claim 1 wherein the step of validating the certificate comprises the further steps of:

comparing the public key included in the response received from the certificate authority filter with a public key included in a response from a second certificate authority filter; and

validating the certificate if the public key included in the response received from the certificate authority filter is the same as the public key received in the response from the second certificate authority filter.

7. A method, in a certificate authority filter connected to a network, for filtering certificates issued from one or more certificate authorities, the method comprising the steps of:

receiving a request comprising an identification of a certificate authority;

identifying the certificate authority in said request;

finding in a table the certificate authority, the table comprising: identification of at least one certificate

authority and a level of trust and a public key associated with each of said at least one certificate authority;

5 determining a level of trust of the identified certificate authority referring to said table;

retrieving a public key associated with the identified certificate authority referring to said table; and

10 sending a response to an originator of the request, said response comprising the level of trust of the identified certificate authority and the public key associated with the identified certificate authority.

8. The method according to claim 7 wherein said request further comprises an identification of a destination entity.

9. The method according to claim 8, wherein:

the table further includes, associated with the certificate authority, the destination entity and a level of trust associated with the destination entity; and

20 wherein the step of determining the level of trust further includes the step of determining the level of trust associated with the destination entity by referring to the table.